WHAT IS CLAIMED IS:

1. A method of community separation control in a Multi-Community Node (MCN), said method comprising:

   determining a first packet community set (PCS) of a first data packet;

   discarding said first data packet in response to detecting said first PCS is null; and

   processing said first data packet in response to detecting said first PCS is not null.

2. The method of claim 1 further comprising recording an event corresponding to said first data packet in response to detecting said PCS is null.

3. The method of claim 1, wherein said determining comprises calculating the intersection of a source network address community set (NACS) of said first data packet and a destination NACS of said first data packet.

4. The method of claim 3, wherein said first data packet is an incoming data packet received on a network interface of said MCN, and wherein said processing comprises:

   discarding said first data packet in response to detecting an interface community set (IFCS) of the interface on which said first data packet was received is not a superset of said PCS; and

   allowing receive processing of said first data packet in response to detecting said IFCS is a superset of said PCS.

5. The method of claim 3, wherein said first data packet is an outgoing data packet to be transmitted on a network interface of said MCN, and wherein said processing comprises:

discarding said first data packet in response to detecting an IFCS of said network interface is not a superset of said PCS, and

allowing transmission of said first data packet in response to determining that said IFCS of said network interface on which said first data packet is to be output is a superset of said PCS.

6. The method of claim 1 further comprising consulting a Community Information Base (CIB).

7. The method of claim 6, wherein said CIB includes community set information corresponding to each IFCS of said MCN, each NACS of said MCN, and the NACS of each node with which said MCN communicates.

8. The method of claim 3, wherein said first data packet is an incoming data packet received on a network interface of said MCN, and wherein said processing comprises:

discarding said first data packet in response to detecting a virtual private network community set (VPNCS) of the interface on which said first data packet was received is not a superset of said PCS; and

allowing receive processing of said first data packet in response to detecting said VPNCS is a superset of said PCS.

9. The method of claim 3, wherein said first data packet is an outgoing data packet to be transmitted on a network interface of said MCN, and wherein said processing comprises:

discarding said first data packet in response to detecting a VPNCS of said network interface is not a superset of said PCS, and

allowing transmission of said first data packet in response to determining that a VPNCS of a network interface on which said first data packet is to be output is a superset of said PCS.

10. A method of community separation control in a closed Multi-Community Node (MCN), said method comprising:

validating a first and second network address of a first data packet;

discarding said first data packet in response to detecting said first network address is not validated or said second network address is not validated; and

processing said first data packet in response to detecting both said first and said second network addresses are validated.

11. The method of claim 10 further comprising recording an event corresponding to said first data packet in response to detecting said network address is not validated.

12. The method of claim 10, wherein said first network address is a source network address and said second network address is a destination network address.

13. The method of claim 12, wherein said first data packet is an incoming data packet, and wherein validating said first network address of said first data packet comprises

determining said first network address is a member of an Attached Address Set (AAS) corresponding to the interface over which said first data packet was received.

14. The method of claim 12, wherein said first data packet is an incoming data packet, and wherein validating said second network address comprises determining that said second network address of said first data packet is a member of the Peer Address Set (PAS) corresponding to the interface over which said first data packet was received.

15. The method of claim 12, wherein said first data packet is an outgoing data packet, and wherein validating said first network address of said first data packet comprises determining that said first network address is a member of the PAS corresponding to the interface over which said first data packet is to be transmitted.

16. The method of claim 12, wherein said first data packet is an outgoing data packet, and wherein validating said second network address comprises determining that said second network address is a member of the AAS corresponding to the interface over which said first data packet is to be transmitted.

17. The method of claim 10 further comprising consulting a Community Information Base (CIB).

18. The method of claim 17, wherein said CIB includes for each network interface on said MCN an AAS and a PAS, wherein said AAS includes the network addresses of nodes on networks attached to or reachable from said network interface of said MCN, and wherein the PAS includes the network addresses of nodes with which nodes whose addresses are in the AAS may communicate, and wherein said method further comprises querying said CIB.

19. A multi-community node comprising:

a processing unit, wherein said processing unit is configured to determine a first packet community set (PCS) of a first data packet, discard said first data packet in response to detecting said first PCS is null, and process said first data packet in response to detecting said first PCS is not null; and

a community information base coupled to said processing unit.

20. The node of claim 19, wherein said processing unit is configured to determine said PCS by calculating the intersection of a source network address community set (NACS) of said first data packet and a destination NACS of said first data packet.

21. The node of claim 19, wherein said first data packet is an incoming data packet received on a network interface of said MCN, and wherein said node is configured to process said first data packet by:

discarding said first data packet in response to detecting an interface community set (IFCS) of the interface on which said first data packet was received is not a superset of said PCS; and

allowing receive processing of said first data packet in response to detecting said IFCS is a superset of said PCS.

22. The node of claim 19, wherein said first data packet is an outgoing data packet to be transmitted on a network interface of said MCN, and wherein said node is configured to process said first data packet by:

discarding said first data packet in response to detecting said IFCS of said network interface is not a superset of said PCS, and

allowing transmission of said first data packet in response to determining that an IFCS of a network interface on which said first data packet is to be output is a superset of said PCS.

23. The node of claim 19, wherein said CIB includes community set information corresponding to each IFCS of said MCN, each NACS of said MCN, and the NACS of each node with which said MCN communicates.

24. The node of claim 19, wherein said first data packet is an incoming data packet received on a network interface of said MCN, and wherein said node is configured to process said first data packet by:

discarding said first data packet in response to detecting a virtual private network community set (VPNCS) of the interface on which said first data packet was received is not a superset of said PCS; and

allowing receive processing of said first data packet in response to detecting said VPNCS is a superset of said PCS.

25. The node of claim 19, wherein said first data packet is an outgoing data packet to be transmitted on a network interface of said MCN, and wherein said node is configured to process said first data packet by:

discarding said first data packet in response to detecting a VPNCS of said network interface is not a superset of said PCS; and

allowing transmission of said first data packet in response to determining that a VPNCS of a network interface on which said first data packet is to be output is a superset of said PCS.

26. A multi-community node comprising:

a processing unit, wherein said processing unit is configured to validate a first and second network address of a first data packet, discard said first data packet in response to detecting said first network address is not validated or said second network address is not validated, and process said first data packet in response to detecting both said first and said second network addresses are validated; and

a community information base coupled to said processing unit.

27. The node of claim 26 wherein said processing unit is further configured to record an event corresponding to said first data packet in response to detecting either said first network address or said second network address is not validated.

28. The node of claim 26, wherein said first network address is a source network address and said second network address is a destination network address.

29. The node of claim 28, wherein said first data packet is an incoming data packet, and wherein said processing unit is configured to validate said first network address of said first data packet by determining said first network address is a member of an Attached Address Set (AAS) corresponding to the interface over which said first data packet was received.

30. The node of claim 28, wherein said first data packet is an incoming data packet, and wherein said processing unit is configured to validate said second network address by determining that said second network address of said first data packet is a member of a Peer Address Set (PAS) corresponding to the interface over which said first data packet was received.

31. The node of claim 28, wherein said first data packet is an outgoing data packet, and wherein said processing unit is configured to validate said first network address of said first data packet by determining that said first network address is a member of the PAS corresponding to the interface over which said first data packet is to be transmitted.

32. The node of claim 28, wherein said first data packet is an outgoing data packet, and wherein said processing unit is configured to validate said second network address comprises by that said second network address is a member of the AAS corresponding to the interface over which said first data packet is to be transmitted.

33. The node of claim 26, wherein said CIB includes for each network interface on said MCN an AAS and a PAS, wherein said AAS includes the network addresses of nodes on networks attached to said network interface of said MCN, and wherein the PAS includes the network addresses of nodes with which nodes whose addresses are in the AAS may communicate, and wherein said processing unit is configured to query said CIB.

34. A computer network comprising:

a multi-community node (MCN), wherein said node comprises:

a processing unit configured to determine a first packet community set (PCS) of a first data packet, discard said first data packet in response to detecting said first PCS is null, and process said first data packet in response to detecting said first PCS is not null, and

a community information base coupled to said processing unit;

a first computer network coupled to said MCN; and

a second computer network coupled to said MCN.

35. The computer network of claim 34, wherein said processing unit is configured to determine said PCS by calculating the intersection of a source network address community set (NACS) of said first data packet and a destination NACS of said first data packet.

36. The computer network of claim 35, wherein said first data packet is an incoming data packet received from said first computer network on a network interface of said MCN, and wherein said processing unit is configured to process said first data packet by:

discarding said first data packet in response to detecting an interface community set (IFCS) of the interface on which said first data packet was received is not a superset of said PCS; and

allowing receive processing of said first data packet in response to detecting said IFCS is a superset of said PCS.

37. The computer network of claim 35, wherein said first data packet is an outgoing data packet to be transmitted to said second computer network on a network interface of said MCN, and wherein said processing unit is configured to process said first data packet by:

discarding said first data packet in response to detecting said IFCS of said network interface is not a superset of said PCS, and

allowing transmission of said first data packet in response to determining that an IFCS of a network interface on which said first data packet is to be output is a superset of said PCS.

38. The computer network of claim 35, wherein said CIB includes community set information corresponding to each IFCS of said MCN, each NACS of said MCN, and the NACS of each node with which said MCN communicates, and wherein said processing unit is configured to query said CIB.

39. The computer network of claim 35, wherein said first data packet is an incoming data packet received from said first computer network on a network interface of said MCN, and wherein said node is configured to process said first data packet by:

discarding said first data packet in response to detecting a VPNCS of the interface on which said first data packet was received is not a superset of said PCS; and

allowing receive processing of said first data packet in response to detecting said VPNCS is a superset of said PCS.

40. The computer network of claim 35, wherein said first data packet is an outgoing data packet to be transmitted to said second computer network on a network interface of said MCN, and wherein said node is configured to process said first data packet by:

discarding said first data packet in response to detecting a VPNCS of said network interface is not a superset of said PCS; and

allowing transmission of said first data packet in response to determining that said VPNCS is a superset of said PCS.

41. A computer network comprising:

a multi-community node (MCN), wherein said node comprises:

a processing unit, wherein said processing unit is configured to validate a first and second network address of a first data packet, discard said first data packet in response to detecting said first network address is not validated or said second network address is not validated, and process said first data packet in response to detecting both said first and said second network addresses are validated, and

a community information base coupled to said processing unit;

a first computer network coupled to said MCN; and

a second computer network coupled to said MCN.

42. The computer network of claim 41 wherein said processing unit is further configured to record an event corresponding to said first data packet in response to detecting either said first network address or said second network address is not validated.

43. The computer network of claim 41, wherein said first network address is a source network address and said second network address is a destination network address.

44. The computer network of claim 43, wherein said first data packet is an incoming data packet, and wherein said processing unit is configured to validate said first network address of said first data packet by determining said first network address is a member of an Attached Address Set (AAS) corresponding to the interface over which said first data packet was received.

45. The computer network of claim 43, wherein said first data packet is an incoming data packet, and wherein said processing unit is configured to validate said second network address by determining that said second network address of said first data

packet is a member of a Peer Address Set (PAS) corresponding to the interface over which said first data packet was received.

46. The computer network of claim 43, wherein said first data packet is an outgoing data packet, and wherein said processing unit is configured to validate said first network address of said first data packet by determining that said first network address is a member of the PAS corresponding to the interface over which said first data packet is to be transmitted.

47. The computer network of claim 43, wherein said first data packet is an outgoing data packet, and wherein said processing unit is configured to validate said second network address comprises by that said second network address is a member of the AAS corresponding to the interface over which said first data packet is to be transmitted.

48. The computer network of claim 41, wherein said CIB includes for each network interface on said MCN an AAS and a PAS, wherein said AAS includes the network addresses of nodes on networks attached to said network interface of said MCN, and wherein the PAS includes the network addresses of nodes with which nodes whose addresses are in the AAS may communicate, and wherein said processing unit is configured to query said CIB.

49. A method of community separation control in a Multi-Community Node (MCN), said method comprising:

ensuring routing table compliance with a community separation policy, wherein all routing table updates are validated to ensure said compliance; and

validating a data packet;

allowing further processing of said data packet in response to detecting said data packet is validated; and

discarding said data packet in response to detecting said data packet is not validated.

50. The method of claim 49, wherein said validating said updates comprises:

determining a network interface through which a next hop corresponding to an update of said updates will be reached;

determining whether a first address corresponding to said next hop is within a first address set of said network interface;

discarding said update in response to determining said destination address is not within said first address set; and

performing said update in response to determining said destination address is within said first address set.

51. The method of claim 50, wherein said network interface is said determined by either extracting an identification of said network interface from said update or by finding a network interface whose network address prefix matches that of said next hop.

52. The method of claim 50, wherein said first address is a destination address and said first address set is an Attached Address Set.

53. The method of claim 50, wherein said first address is a Network Address Community Set (NACS) corresponding to a destination address of said next hop, and wherein said first address set is an Interface Community Set (IFCS) of said network interface.

54. The method of claim 50, wherein said data packet is an outgoing data packet, and wherein validating said data packet comprises:

determining said destination address is reachable; and

determining a community set corresponding to an interface over which said data packet is to be output includes a community set corresponding to said destination address.

55. The method of claim 50, wherein said data packet is an incoming data packet, and wherein validating said data packet comprises checking that a source address of said data packet is within an AAS of the interface over which said data packet was received.

56. The method of claim 50, wherein said data packet is received on a first interface of said MCN and is to be forwarded to a second interface of said MCN, and wherein validating said data packet comprises determining an intersection of an Interface Community Set (IFCS) of said first interface with an IFCS of said second interface is not null.

57. The method of claim 49 further comprising consulting a Community Information Base (CIB).

58. The method of claim 57, wherein said CIB includes an IFCS corresponding to each interface of said MCN, and an AAS corresponding to each interface of said MCN indicating destination addresses or destination subnets which are reachable through each of said interfaces.

59. The method of claim 50, further comprising recording an event corresponding to said update in response to determining said destination address is not within said first address set.

60. A multi-community node comprising:

a processing unit, wherein said processing unit is configured to ensure routing table compliance with a community separation policy, wherein all routing table updates are validated to ensure said compliance, validate a data packet, allow further processing of said data packet in response to detecting said data packet is validated, and discard said data packet in response to detecting said data packet is not validated; and

a community information base (CIB) coupled to said processing unit.

61. The node of claim 60, wherein in validating said updates said processing unit is configured to:

determine a network interface through which a next hop corresponding to an update of said updates will be reached;

determine whether a first address corresponding to said next hop is within a first address set of said network interface;

discard said update in response to determining said destination address is not within said first address set; and

perform said update in response to determining said destination address is within said first address set.

62. The node of claim 61, wherein said network interface is said determined by either extracting an identification of said network interface from said update or by finding a network interface whose network address prefix matches that of said next hop.

63. The node of claim 61, wherein said first address is a destination address and said first address set is an Attached Address Set.

64. The node of claim 61, wherein said first address is a Network Address Community Set (NACS) corresponding to a destination address of said next hop, and wherein said first address set is an Interface Community Set (IFCS) of said network interface.

65. The node of claim 61, wherein said data packet is an outgoing data packet, and wherein in validating said data packet said processing unit is configured to:

determine said destination address is reachable; and

determine a community set corresponding to an interface over which said data packet is to be output includes a community set corresponding to said destination address.

66. The node of claim 61, wherein said data packet is an incoming data packet, and wherein validating said data packet comprises checking that a source address of said data packet is within an AAS of the interface over which said data packet was received.

67. The node of claim 61, wherein said data packet is received on a first interface of said MCN and is to be forwarded to a second interface of said MCN, and wherein validating said data packet comprises determining an intersection of an Interface Community Set (IFCS) of said first interface with an IFCS of said second interface is not null.

68. The node of claim 60 further comprising consulting said CIB.

69. The node of claim 68, wherein said CIB includes an IFCS corresponding to each interface of said MCN, and an AAS corresponding to each interface of said MCN indicating destination addresses or destination subnets which are reachable through each of said interfaces.

70. The node of claim 61, further comprising recording an event corresponding to said update in response to determining said destination address is not within said first address set.

71. A computer network comprising:

a multi-community node (MCN), wherein said node comprises:

a processing unit, wherein said processing unit is configured to ensure routing table compliance with a community separation policy, wherein all routing table updates are validated to ensure said compliance, validate a data packet, allow further processing of said data packet in response to detecting said data packet is validated, and discard said data packet in response to detecting said data packet is not validated; and

a community information base (CIB) coupled to said processing unit;

a first computer network coupled to said MCN; and

a second computer network coupled to said MCN.

72. The computer network of claim 71, wherein in validating said updates said node is configured to:

determine a network interface through which a next hop corresponding to an update of said updates will be reached;

determine whether a first address corresponding to said next hop is within a first address set of said network interface;

discard said update in response to determining said destination address is not within said first address set; and

perform said update in response to determining said destination address is within said first address set.

73. The computer network of claim 72, wherein said node is configured to determine said network interface by either extracting an identification of said network interface from said update or by finding a network interface whose network address prefix matches that of said next hop.

74. The computer network of claim 72, wherein said first address is a destination address and said first address set is an Attached Address Set.

75. The computer network of claim 72, wherein said first address is a Network Address Community Set (NACS) corresponding to a destination address of said next hop, and wherein said first address set is an Interface Community Set (IFCS) of said network interface.

76. The computer network of claim 72, wherein said data packet is an outgoing data packet originating in said MCN, and wherein in validating said data packet said node is configured to:

determine said destination address is reachable; and

determine a community set corresponding to an interface over which said data packet is to be output includes a community set corresponding to said destination address.

77. The computer network of claim 72, wherein said data packet is an incoming data packet from said first computer network, and wherein validating said data packet comprises checking that a source address of said data packet is within an AAS of the interface over which said data packet was received.

78. The computer network of claim 72, wherein said data packet is received on a first interface of said MCN and is to be forwarded to a second interface of said MCN, wherein said first interface corresponds to said first computer network and said second interface corresponds to said second computer network, and wherein in validating said data packet said node is configured to determine that an intersection of an Interface Community Set (IFCS) of said first interface with an IFCS of said second interface is not null.

79. The computer network of claim 71, further comprising consulting said CIB.

80. The computer network of claim 79, wherein said CIB includes an IFCS corresponding to each interface of said MCN, and an AAS corresponding to each interface of said MCN indicating destination addresses or destination subnets which are reachable through each of said interfaces.

81. The computer network of claim 72, further comprising recording an event corresponding to said update in response to determining said destination address is not within said first address set.